1:20 MJ 9150

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jason M. Guyton, being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the Department of Homeland Security (DHS), Homeland Security Investigations (HSI), currently assigned to HSI Cleveland, Ohio. I have been employed since March 2009. As part of my daily duties as an HSI Special Agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2251(a), 2252(a) and 2252A(a). I have received training in child pornography and child exploitation investigations and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.

2. The statements in this affidavit are based upon my personal knowledge and observations, my training and experience, information obtained from other law enforcement and witnesses, and the review of various documents and records. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth the facts that I believe necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a) are present in the information associated with the account **daufap@yahoo.com**. I make this affidavit in support of an application for a search warrant for content and records associated with the above account which is stored at a premises owned, maintained, controlled, or operated by Oath Holdings Inc. ("Oath") (formerly Yahoo Holdings, Inc.), an e-mail, remote storage and software provider headquartered at 701 First Avenue,

Sunnyvale, CA 94089.

3. The information and account to be searched is described in the following paragraphs and in Attachments A and B. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Oath to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the account referenced in this affidavit and further in Attachment A, including the contents of the communications.

4. I have probable cause to believe that evidence of violations of 18 U.S.C. § 2252A, involving the use of a computer in or affecting interstate commerce to transport, receive, distribute, possess and/or access child pornography is located within the aforementioned account described below. I have reason to believe that the member account that is the subject of the instant application will have stored information and communications that are relevant to this investigation, to include evidence of the identity of the person maintaining the account and other relevant information associated with the user. Thus, as outlined below, and based on my training and experience, there is probable cause to believe that evidence, fruits and/or instrumentalities of the crimes are in this account.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of Title 18, United States Code, §2252A, and relating to material involving the sexual exploitation of minors. 18 U.S.C. § 2252A prohibits a person from knowingly mailing, transporting, shipping, distributing, receiving, reproducing for distribution, possessing or accessing with intent to view any child pornography, as defined in 18 U.S.C. §2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such

child pornography was produced using materials that had traveled in interstate or foreign commerce.

6. The legal authority for this search warrant application is derived from Title 18, United States Code, chapter 121, §§ 2701-11, entitled "Stored Wire and Electronic Communications and Transactional Records Access." 18 U.S.C. § 2703(c)(A) allows for nationwide service of process of search warrants for the contents of electronic communications. Pursuant to 18 U.S.C. § 2703, as amended by the USA PATRIOT Act, Section 220, a government entity may require a provider of an electronic communication service or a remote computing service to disclose a record or other information pertaining to a subscriber or customer of such service pursuant to a warrant issued using procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation. 18 U.S.C. § 2510(12) defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo optical system that affects interstate or foreign commerce," with certain exceptions not applicable here. 18 U.S.C. § 2510(17) defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."

DEFINITIONS

7. The following definitions apply to this Affidavit and its Attachments:

a. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes

undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

c. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

d. The term "child pornography," as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where

i. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

ii. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

iii. such visual depiction has been created, adapted, or modified to

appear that an identifiable minor is engaging in sexually explicit conduct.

e. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as flash drives, SD cards, floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), optical disks, printer buffers, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

f. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

g. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies a computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can

be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. A creation IP address is the address used on the date that an e-mail account is created by the user.

h. "Domain names" are common, easy to remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

i. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

j. A "Preservation Letter" is a letter governmental entities may issue to Internet providers pursuant to 18 U.S.C. § 2703(f) to ensure that the Internet Providers preserve records in its possession. The preservation of such records is necessary given the dynamic nature of digital records that may be deleted.

k. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

l. A "hash value" is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file's content. A

hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.

INFORMATION ABOUT OATH HOLDINGS INC.

8. In my training and experience, I have learned that Oath provides a variety of on-line services, including electronic mail ("email") access, to the public. Specifically, Oath allows subscribers to obtain email accounts at the domain name @yahoo.com, like the email account that is the subject of this warrant.

9. Subscribers obtain an account by registering with Oath. During the registration process Oath asks subscribers to provide basic personal information. Therefore, the computers of Oath are likely to contain stored electronic communications (including retrieved and un-retrieved email for subscribers) and information concerning subscribers and their use of services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

7. An Oath subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Oath. In addition, Oath maintains a messaging application service.

8. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

9. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity this information often provides clues to their identity, location, or illicit activities.

10. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the IP address used to register the account and the IP addresses associated with logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

11. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user because of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

12. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contact lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time.

13. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the IP addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of

the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications to conceal them from law enforcement).

14. I know from my training and experience that Oath preserves the content of the accounts that have been flagged, or at the request of a law enforcement agency preservation request.

CURRENT INVESTIGATION

Initiation of Investigation and Probable Cause

15. On May 4, 2020, the Electronic Service Provider (ESP) Oath Holding Inc. (formerly known as Yahoo) submitted Cyber Tipline Report 71606471 to the National Center for Missing and Exploited Children (NCMEC) regarding the possible possession, manufacture, and/or distribution of child pornography by the following user:

Name:	Tom Doer
Phone:	n/a
Email Address:	**daufap@yahoo.com**
ESP User ID:	RGQXX2MYHJVIQ65YG262CHWWUI
Alternate Email:	jake6734@gmail.com

16. Oath reported that on April 30, 2020, this user uploaded 355 files of apparent child pornography over the Yahoo Mail platform. Oath reported these files were uploaded on April 30, 2020 at 07:35pm (UTC) from IP address 2600:1009:b045:40bf:ccd7:e108:a493:1124. Oath, after viewing the content of these files, provided them all to NCMEC as part of their Cyber Tip Report.

17. NCMEC reviewed the Cyber Tip Report and after conducting research determined that this activity likely occurred in the area of Cleveland, Ohio based on the reported IP address. On May

5, 2020, NCMEC routed this report to the Ohio Internet Crimes Against Children (ICAC) Task Force.

18. On May 5, 2020, Ohio ICAC Task Force Investigator Beth Crano served a Cuyahoga County Grand Jury subpoena on Verizon for subscriber information related to IP address 2600:1009:b045:40bf:ccd7:e108:a493:1124 on April 30, 2020 at 07:35pm UTC.

19. On May 12, 2020, Oath submitted Cyber Tip Report 72158943 to NCMEC as an escalation/supplemental to Cyber Tip Report 71606471. Oath reported that based on the login records and subscriber information for **daufap@yahoo.com** along with open source research, the user appears to be an individual named **William Dale SCHAFFER**, residing in or around Wellington, Ohio. Oath further reported that an investigation by their Verizon Media E-Crime Investigations Team (VM-ECIT) revealed that **SCHAFFER** appears to work as a Firefighter/EMT/Driver-engineer at the Elyria Fire Department.

20. The VM-ECIT confirmed that the last successful login to the **daufap@yahoo.com** account was on April 30, 2020, from a Verizon Wireless IP address located in or around Cleveland, Ohio. This login was associated with the b-cookie "e1501r8hr9jiu". VM-ECIT reported that **daufap@yahoo.com** is associated with two (2) additional Yahoo accounts based on this b-cookie: willfire67@yahoo.com and wilma67@yahoo.com. The user provided information for willfire67@yahoo.com is:

> Name: Bob Shoemaker
> Phone: 1-4402131618 (Verified)
> Account Created: 11/07/2015 Grafton, Ohio

On April 30, 2020, willfire67@yahoo.com successfully logged into their account from the same IP address that **daufap@yahoo.com** used on that day.

21. On May 6, 2020, VM-ECIT queried the verified phone number (440-213-1618) provided by willfire67@yahoo.com in the TLO (TransUnion) database and found that number was associated with **William Dale SCHAFFER** (DOB: XX/XX/1967) with possible addresses in Wellington, Grafton, and Elyria, Ohio. The TLO report further indicated that **SCHAFFER** was possibly associated with multiple email addresses to include willfire67@yahoo.com.

22. On May 6, 2020, VM-ECIT queried Spokeo using email addresses associated with **SCHAFFER** and located the Facebook profile: https://www.facebook.com/bill.schaffer.946. The name on this Facebook profile is "Bill Schaffer" and in the "About" section it lists works as Maintenance/Groundskeeper at Lorain County Speedway and Firefighter/EMT/Driver-engineer at Elyria Fire Department. Spokeo also located the Twitter profile: https://twitter.com/willfire67. The name on the Twitter profile is "Bill Schaffer" and in the "Work" section it lists profession firefighter/EMT. VM-ECIT reported that images of the male observed on the Facebook and Twitter profiles match non-reported images of a male they observed in the **daufap@yahoo.com** account. VM-ECIT indicated that the non-reported images in this Yahoo account can be provided to law enforcement with appropriate legal process.

23. NCMEC reviewed Cyber Tip Report 72158943 and after conducting research determined that it was associated with Cyber Tip 71606471. On May 18, 2020, NCMEC routed this report to the Ohio ICAC Task Force.

24. On May 19, 2020, Investigator Crano queried the Ohio Law Enforcement Gateway (OHLEG) database for William Dale SCHAFFER and found and Ohio driver's license for an individual with that name listing a date of birth of XX/XX/1967, a social security number of XXX-XX-4649, and a current residential address of XXXXX Webster Road, Wellington, Ohio 44090 .

25. On May 21, 2020, the Ohio ICAC Task Force provided the Cyber Tip Reports and corresponding investigative findings to HSI Cleveland. On May 26, 2020, your Affiant submitted a preservation of records request to Oath for all available content associated with the email accounts **daufap@yahoo.com**, willfire67@yahoo.com, and wilma6710@yahoo.com. Your Affiant reviewed the Facebook and Twitter accounts associated with "Bill Schaffer" and verified they listed firefighter/EMT. Your Affiant further observed multiple pictures of an adult male on these accounts that match the pictures of **SCHAFFER** in the OHLEG database.

26. On May 26, 2020, your Affiant viewed the 355 files provided by Oath as part of the Cyber Tip Reports. The files include 346 images and nine (9) videos, the majority of which depict suspected child exploitation material involving children with ages ranging from toddler to young teen. Most of the children appear to be under the age of thirteen (13) and include multiple toddlers. Four (4) of these files can be more fully described as follows:

- *image.116-1.jpeg – this image file depicts a naked prepubescent (approximately 5-6 years old) female positioned in a bathtub between the legs of an adult male. The child's left hand is on the male's erect penis and she is inserting it into her mouth. The child's face is visible.*
- *image.297-1.jpeg – this image file depicts a naked prepubescent (approximately 5-6 years old) female sitting in a chair with her legs spread while what appears to be an adult's finger is inserted into her vagina. The camera is focused on the act and no faces are visible.*
- *image.883-1.jpeg – this image file depicts a naked prepubescent (approximately 9-10 years old) female sitting on the floor and leaning backward against a cupboard with her legs spread. The child is using her right hand to insert what appears to be a sex toy into her vagina and her face is visible.*

- *video.75-1.jpeg – this 45 second video file depicts a naked prepubescent (approximately 10-12 years old) male and a naked prepubescent (approximately 10-12 years old) female engaging in genital to genital sexual intercourse. What appears to be an adult hand reaches from behind the camera and assists the male child with inserting his penis into the female child's vagina. As the act continues, the individual filming backs away and the male child's face is visible. The video did not contain any audio.*

27. On May 27, 2020, in response to the Cuyahoga County Grand Jury subpoena (Paragraph 18), Verizon Wireless confirmed that on April 30, 2020 IP address 2600:1009:b045:40bf:ccd7:e108:a493:1124 was associated with the cellphone number 440-213-1618. Verizon provided the following subscriber information related to the phone number 440-213-1618:

Account Number: 481804807-1
Last Name: SCHAFFER
First Name: William
Address: 43421 Webster Rd
City: Wellington
State: OH
Zip Code: 44090-9037
Activation Date: 1/20/1998 (STILL ACTIVE)

28. Based on the information above, I believe **SCHAFFER** was in the Northern District of Ohio at the time he used his email account to possess and/or distribute child pornography.

29. Based on the above information, I have probable cause to believe that the user of the **daufap@yahoo.com** committed the offense of possessing, receiving, and/or distributing child pornography, in violation of Title 18, United States Code, §§2252A and that information contained within this account and maintained at Oath will assist myself and law enforcement in identifying the person or persons using this account.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

30. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Oath to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

31. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the computer systems in control of Oath there exists evidence of a crime, contraband and/or fruits of a crime. Based on the aforementioned information, I respectfully submit that there is probable cause to believe that the Oath email account described in Attachment A will contain evidence of a crime, specifically but not limited to, identification of the person who possessed and/or distributed files of child pornography through the Oath account discussed above. Accordingly, a search warrant is requested.

32. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(I).

33. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Because the warrant will be served on Oath Holding, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Jason M. Guyton
Special Agent
Homeland Security Investigations

Sworn to via telephone after submission by reliable electronic means [Fed. R. Crim. P. 4.1 and 41(d)(3)] on this 29th day of May 2020.

WILLIAM H. BAUGHMAN, JR.
UNITED STATES MAGISTRATE JUDGE